Exhibit B

EFF's History

Staff

Board of Directors

Advisory Board

Special Counsel & Special Advisors

Reports and Financials

Interns and External Fellowships

Opportunities

- Job Openings
- Legal Interns
- Tech Interns
- Volunteer

Contact EFF

- Legal Assistance from EFF
- Report Security Vulnerabilities to EFF

About EFF

The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. We work to ensure that rights and freedoms are enhanced and protected as our use of technology grows.

Even in the fledgling days of the Internet, EFF understood that protecting access to developing technology was central to advancing freedom for all. In the years that followed, EFF used our fiercely independent voice to clear the way for open source software, encryption, security research, file sharing tools, and a world of emerging technologies.

Today, EFF uses the unique expertise of leading technologists, activists, and attorneys in our efforts to defend free speech online, fight illegal surveillance, advocate for users and innovators, and support freedom-enhancing technologies.

Together, we forged a vast network of concerned members and partner organizations spanning the globe. EFF advises policymakers and educates the press and the public through comprehensive analysis, educational guides, activist workshops, and more. EFF empowers hundreds of thousands of individuals through our Action Center and has become a leading voice in online rights debates.

EFF is a donor-funded US 501(c)(3) nonprofit organization that depends on your support to continue fighting for users.

Additional information:

- Become an EFF member
- View our annual reports and financial information
- Historic EFF court victories
- EFF's founding

Donate to EFF

Stay in Touch

Email Address

Postal Code (optional)

SIGN UP NOW

NSA Spying

eff.org/nsa-spying

EFF is leading the fight against the NSA's illegal mass surveillance program. Learn more about what the program is, how it works, and what you can do.

Follow EFF

The EFF crew is heading to Brussels! Join us for a Speakeasy meetup on Tuesday night. https://www.eff.org/r.n4sp

JAN 21 @ 11:48PM

Friday keynote at #SCALE14x: fighting the war on general purpose computing with @doctorow. https://eff.org/scale14x

JAN 21 @ 9:14PM

Copyright law creates a legal fence between you and ownership of your digital goods. @CenDemTech for #CopyrightWeek: https://cdt.org/blog/ownershi

JAN 21 @ 5:45PM

Twitter Facebook Identi.ca

Projects

Bloggers' Rights

Coders' Rights

Free Speech Weak Links

Global Chokepoints

HTTPS Everywhere

Manila Principles

Medical Privacy Project

Open Wireless Movement

Patent Busting

Privacy Badger

Student Activism

Student Privacy

Surveillance Self-Defense

Takedown Hall of Shame

Teaching Copyright

Transparency Project

Trolling Effects

Ways To Help

EFF's History
Staff
Board of Directors
Advisory Board
Special Counsel & Special Advisors
Reports and Financials
Interns and External Fellowships
Opportunities
Job Openings
Legal Interns
Tech Interns
Volunteer
Contact EFF
Legal Assistance from EFF
Report Security Vulnerabilities to EFF

A History of Protecting Freedom Where Law and Technology Collide

The Electronic Frontier Foundation was founded in July of 1990 in response to a basic threat to speech. The United States Secret Service conducted a series of raids tracking the distribution of a document illegally copied from a BellSouth computer that described how the emergency 911 system worked, referred to as the E911 document. The Secret Service believed that if "hackers" knew how to use the telephone lines set aside for receiving emergency phone calls, the lines would become overloaded and people facing true emergencies would be unable to get through.

One of the alleged recipients of the E911 document was the systems operator at a small games book publisher out of Austin, Texas, named Steve Jackson Games. The Secret Service executed a warrant against the innocent Jackson and took all electronic equipment and copies of an upcoming game book from Steve Jackson Games's premises. Steve Jackson panicked as he watched the deadline come and go for his latest release and still hadn't received his computers back. He was forced to lay off nearly half of his staff. In the end, the Secret Service returned all of Steve Jackson's computers and decided not to press charges against the company, since they were unable to find any copies of the E911 document on any of the computers.

In the meantime, Steve Jackson's business was nearly ruined. And when he and his employees had the opportunity to investigate the returned computers, they noticed that all of the electronic mail that had been stored on the company's electronic bulletin board computer, where non-employee users had dialed in and sent personal messages to one another, had been individually accessed and deleted. Steve Jackson was furious, as he believed his rights as a publisher had been violated and the free speech and privacy rights of his users had been violated. Steve Jackson tried desperately to find a civil liberties group to help him, to no avail. Unfortunately, none of the existing groups understood the technology well enough to understand the importance of the issues.

In an electronic community called the Whole Earth 'Lectronic Link (now WELL.com) several informed technologists understood exactly what civil liberties issues were involved. Mitch Kapor, former president of Lotus Development Corporation, John Perry Barlow, Wyoming cattle rancher and lyricist for the Grateful Dead, and John Gilmore, an early employee of Sun Microsystems, decided to do something about it. They formed an organization to work on civil liberties issues raised by new technologies. And on the day they formally announced the organization, they announced that they were representing Steve

Jackson Games and several of the company's bulletin board users in a lawsuit they were bringing against the United States Secret Service. The Electronic Frontier Foundation was born!

The Steve Jackson Games case turned out to be an extremely important one in the development of a proper legal framework for cyberspace. For the first time, a court held that electronic mail deserves at least as much protection as telephone calls. We take for granted today that law enforcement must have a warrant that particularly describes all electronic mail messages before seizing and reading them. The Steve Jackson Games case established that principle.

The Electronic Frontier Foundation continues to take on cases that set important precedents for the treatment of rights in cyberspace. In our second big case, Bernstein v. U.S. Dept. of Justice, the United States government prohibited a University of California mathematics Ph.D. student from publishing on the Internet an encryption computer program he had created. Years before, the government had placed encryption, a method for scrambling messages so they can only be understood by their intended recipients, on the United States Munitions List, alongside bombs and flamethrowers, as a weapon to be regulated for national security purposes. Companies and individuals exporting items on the munitions list, including software with encryption capabilities, had to obtain prior State Department approval.

Encryption export restrictions crippled American businesses and damaged the free speech rights of individuals. Critical for ecommerce, companies use encryption to safeguard sensitive information, such as credit card numbers, which they send or receive over electronic networks. Companies also secure access to software programs and provide system security using encryption. By limiting the export of encryption, technologies and methods, the U.S. government drove development of security software overseas, where American companies were unable to compete.

The State Department was unsympathetic to Bernstein's situation and told Bernstein he would need a license to be an arms dealer before he could simply post the text of his encryption program on the Internet. They also told him that they would deny him an export license if he actually applied for one, because his technology was too secure.

The Electronic Frontier Foundation pulled together a top-notch legal team and sued the United States government on behalf of Dan Bernstein. The court ruled, for the first time ever, that written software code is speech protected by the First Amendment. The court further ruled that the export control laws on encryption violated Bernstein's First Amendment rights by prohibiting his constitutionally protected speech. As a result, the government changed its export regulations. Now everyone has the right to "export" encryption software -- by publishing it on the Internet -- without prior permission from the U.S. government. Once again, the Electronic Frontier Foundation led the charge to establish important cyberspace rights.

Today's Issues

While early threats to our right to communicate came from the government, current threats come also from industry, as it seeks to control and expand current revenue sources at the expense of traditional fair use. The trend has been for industry to use a

Bloggers' Rights

Coders' Rights

Free Speech Weak Links

Global Chokepoints

HTTPS Everywhere

Manila Principles

Medical Privacy Project

Open Wireless Movement

Patent Busting

Privacy Badger

Student Activism

Student Privacy

Surveillance Self-Defense

Takedown Hall of Shame

Teaching Copyright

Transparency Project

Trolling Effects

Ways To Help

combination of law and technology to suppress the rights of people using technology. Nowhere is this more evident than in the world of copyright law, where the movie and recording studios are trying to dumb down technology to serve their "bottom lines" and manipulate copyright laws to tip the delicate balance toward intellectual property ownership and away from the right to think and speak freely.

CDT is a champion of global online civil liberties and human rights, driving policy outcomes that keep the Internet open, innovative, and free.

At the Center for Democracy & Technology (CDT), we believe in the power of the Internet. Whether it's facilitating entrepreneurial endeavors, providing access to new markets and opportunities, or creating a platform for free speech, the Internet empowers, emboldens and equalizes people around the world.

As a 501(c)(3) nonprofit organization, we work to preserve the user-controlled nature of the Internet and champion freedom of expression. We support laws, corporate policies, and technology tools that protect the privacy of Internet users, and advocate for stronger legal controls on government surveillance.

With offices in Washington, DC and San Francisco, and an international presence in London and Brussels, CDT works inclusively across sectors and the political spectrum to find tangible solutions to today's most pressing Internet policy challenges.

OUR MISSION

ISSUES

CONSUMER PRIVACY

WHO WE ARE

We are a team of experts with deep knowledge of issues pertaining to the Internet, privacy, security, technology, and intellectual property. We come from academia, private enterprise, government, and the non-profit worlds to translate complex policy into action.

OUR STAFF

HISTORY

For the last 20 years, CDT has been working at the forefront of public policy, advancing an open, innovative, and free Internet. CDT's work has led to groundbreaking legislation, landmark court cases, and new industry standards and practices.

HIGHLIGHTS

FINANCIALS

Our funding is diverse, balanced, and impartial.

LEARN MORE

WORKING GROUPS

Exchanging views and seeking actionable solutions.

LEARN MORE

ANNUAL DINNER

The most influential minds of today's tech policy world, the most

pressing issues in the field, and the opportunity to connect with attendees from all sectors. Save the date - Tech Prom is happening April 6, 2016!

LEARN MORE

MISSION & PRINCIPLES

CDT is a champion of global online civil liberties and human rights, dedicated to driving policy outcomes that keep the Internet open, innovative, and free.

We work to:

- Preserve the unique nature of the Internet.
- Enhance freedom of expression globally.
- Protect our fundamental right to privacy.
- Limit government surveillance.
- Define the boundaries of technology in our daily lives.

HOW CDT WORKS

CDT brings together thought leaders to find innovative and practical solutions to the policy challenges surrounding the Internet. We provide leadership and advocacy to help shape public policy and industry best practices, while providing a forum for stakeholder dialogue. This dialogue doesn't always lead to consensus, but it often helps lead to an understanding of contrary points of view, and the collaborative process helps to bring new solutions to the surface. Our current working groups focus on government privacy and security issues; consumer privacy; and free expression.

CDT'S RECORD OF SUCCESS

CDT has spent the last 20 years advocating for groundbreaking legislation, winning landmark court cases, building winning coalitions and promoting industry standards and practices.

VIEW HIGHLIGHTS

CDT'S GOVERNANCE

CDT is governed by an independent Board of Directors. The Board is the sole entity with authority over CDT's operations.

While CDT collaborates with a wide range of Internet stakeholders, it is neither a membership organization nor a trade association. CDT does not represent the interests or views of any company, industry segment, government or any other set of parties.

CDT'S FUNDING

CDT receives support from a wide range of philanthropic foundations, companies, individuals, and court settlements ("cy pres" awards). Financial supporters do not sit on the Board of Directors and have no role in decision-making regarding policy or the organization's oversight.

The **CyLab Usable Privacy and Security Laboratory (CUPS)** brings together researchers working on a diverse set of projects related to understanding and improving the usability of privacy and security software and systems. Our research employs a combination of three high-level strategies to make secure systems more usable: building systems that "just work" without involving humans in security-critical functions; making secure systems intuitive and easy to use; and teaching humans how to perform security-critical tasks.

CUPS is affiliated with Carnegie Mellon CyLab. Our research is funded by grants from the National Science Foundation, the Army Research Lab, Microsoft, and Google. Wombat Security Technologies, Inc. is commercializing some of the technologies we developed.

CUPS students come from several CMU PhD programs including the programs in Societal Computing, Engineering and Public Policy, Human Computer Interaction, Computer Science, Electrical and Computer Engineering, and Public Policy and Management. Prospective students should apply directly to these programs and also express their interest in the CUPS doctoral training program.

News and Events

We celebrated privacy day at CMU on January 28, 2015 with a privacy clinic, privacy research showcase, and keynote talk by FTC Commissioner Julie Brill.

Check out our Privacy Illustrated website featuring illustrations of privacy from kindergartners through adults

Our privacy engineering masters program has graduated its first class. Alumni have accepted jobs at Google, Oracle, Adobe, and Ebay. Applications for fall 2015 are due in January.

Our NSF-sponsored Usable Privacy Policy Project is developing approaches to extracting useful information from natural-language privacy policies and displaying that information in useful ways for users.

We are participating in the ARL Collaborative Research Alliance on cybersecurity

Videos from our June 27, 2014 Workshop on the Future of Privacy Notice and Choice are now available

Check out the July 2015 edition of our lab newsletter, The Saucer.

People

Director: Lorrie Cranor

Current members: Alessandro Acquisti, Yuvraj Agrawal, Hazim

Almuhimedi, Lujo Bauer, Sekhar Bhagvatula, Nicolas Christin, Julie Downs, Alain Forget, David Gordon, Jim Graves, Hanan Hibshi, Candice Hoke, Mandy Holbrook, Jason Hong, Saranga Komanduri, Darya Kurilova, Pedro Leon, Shing-hon Lau, Bin Liu, Abby Marsh, Billy Melicher, Alessandro Oltramari, Emmanuel Owusu, Norman Sadeh, Ashwini Rao, Marios Savvides, Florian Schaub, Sean Segreti, Rich Shay, Stephen Siena, Manya Sleeper, Josh Tan, Yuan Tian, Tiffany Todd, Blase Ur, Timothy Vidas

Alumni and former lab members: Idris Adjerid, Fahd Arshad, Rebecca Hunt Balebako, Cristian Bravo-Lillo, Joanna Bresee, Luc Cesca, Justin Cranshaw, Paul Hankes Drielsma, Adam Durity, Serge Egelman, Ian Fette, Eiji Hayashi, Naoko Hayashida, Philip Huh, Peter Klemperer, Cynthia Kuo, Eduardo A. Cuervo Laffaye, Matthew Geiger, Iulia Ion, Patrick Kelley, Braden Kowitz, Ponnurangam Kumaraguru, Janne Lindqvist, Chris Long, Ryan Mahon, Michelle Mazurek, Aleecia McDonald, Marty McGuire, Jonathan Mugan, Elaine Newton, Greg Norcie, Sven Dietrich, Robert Reeder, Bryan Pendleton, Sasha Romanosky, Steve Sheng, Fred Stutzman, Eran Toch, Janice Tsai, Kami Vaniea, Tatiana Vlahovic, Kai Wang, Yang Wang, Jason Wiese, Shomir Wilson

Current Projects and Selected Publications

Privacy decision making | Passwords and authentication | User controllable security and privacy | Usable cyber trust indicators

Privacy decision making

While most people claim to be very concerned about their privacy, they do not consistently take actions to protect it. Web retailers detail their information practices in their privacy policies, but most of the time this information remains invisible to consumers. Our research focuses on understanding how individuals make privacy-related decisions, finding ways to make privacy information more usable to consumers, and using soft-paternalism to provide privacy nudges. CUPS researchers developed a "nutrition label" for privacy and a search engine for bank privacy policies. We are also studying user attitudes about privacy on social networks, privacy

for mobile apps, and as the usability and effectiveness of online tracking opt-out tools. Our Usable Privacy Policy Project is developing approaches to extracting information from natural-language privacy policies and displaying that information in useful ways for users.

Recent papers

F. Schaub, R. Balebako, A. Durity, and L. Cranor. A Design Space for Effective Privacy Notices. SOUPS 2015.

H. Almuhimedi, F. Schaub, N. Sadeh, I. Adjerid, A. Acquisti, J. Gluck, L. F. Cranor, Y. Agarwal. Your Location has been Shared 5,398 Times!: A Field Study on Mobile App Privacy Nudging. CHI2015.

A. Rao, F. Schaub, N. Sadeh. What do they know about me? Contents and Concerns of Online Behavioral Profiles. PASSAT '14. December 2014. J. R. Reidenberg, T. D. Breaux, L. F. Cranor, B. French, A. Grannis, J. T. Graves, F. Liu, A. M. McDonald, T. B. Norton, R. Ramanath, N. C. Russell, N. Sadeh, F. Schaub. Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding. 42nd Research Conference on Communication, Information and Internet Policy (TPRC '14). September 2014.

L. Cranor, A. Durity, A. Marsh, and B. Ur. Parents' and Teens' Perspectives on Privacy in a Technology-Filled World. SOUPS 2014.

Y. Wang, P. Leon, A. Acquisti, L.F. Cranor, A. Forget, N. Sadeh. A Field Trial of Privacy Nudges for Facebook. ACM SIGCHI Conference on Human Factors in Computing Systems (CHI2014). [teaser video]

Rebecca Balebako, Abigail Marsh, Jialiu Lin, Jason Hong, Lorrie Faith Cranor. The Privacy and Security Behaviors of Smartphone App Developers. Workshop on Usable Security (USEC 2014). San Diego, CA, February 23, 2014.

Rebecca Balebako, Rich Shay, and Lorrie Faith Cranor. Is Your Inseam a Biometric? A Case Study on the Role of Usability Studies in Developing Public Policy. Workshop on Usable Security (USEC 2014). San Diego, CA, February 23, 2014.

>> More privacy decision making papers ...

Passwords and authentication

To combat both the inherent and user-induced weaknesses of text-based passwords, administrators and organizations typically institute a series of rules – a password policy – to which users must adhere when choosing a password. There is consensus in the literature that a properly-written password policy can provide an organization with increased security. There is, however, less accord in describing just what such a well-written policy would be, or even how to determine whether a given policy is effective. Although it is easy to calculate the theoretical password space that corresponds to a particular password policy, it is difficult to determine the practical password space. Users may, for example, react to a policy rule requiring them to include numbers in passwords by overwhelmingly picking the same number, or by always using the number in the same location in their passwords. There is little published empirical research that studies the strategies used by actual users under various password policies. In addition, some password policies, while resulting in stronger passwords, may make those passwords difficult to remember or

type. This may cause users to engage in a variety of behaviors that might compromise the security of passwords, such as writing them down, reusing passwords across different accounts, or sharing passwords with friends. Other undesirable side effects of particular password policies may include frequently forgotten passwords. In fact, the harm caused by users following an onerously restrictive password policy may be greater than the harm prevented by that policy. In this project, we seek to advance understanding of the factors that make creating and following appropriate password policies difficult, collect empirical data on password entropy and memorability under various password policies, and propose password policy guidelines to simultaneously maximize security and usability of passwords. We also explore the security and usability of some new types of passwords.

Recent papers

B. Ur, S. Segreti, L. Bauer, N. Christin, L. Cranor, S. Komanduri, D. Kurilova, M. Mazurek, W. Melicher and R. Shay. Measuring Real-World Accuracies and Biases in Modeling Password Guessability. USENIX Security Symposium 2015. [1-minute lightning talk video]

B. Ur, F. Noma, J. Bees, S. Segreti, R. Shay, L. Bauer, N. Christin, L Cranor. "I Added '!' At The End To Make It Secure": Observing Password Creation in the Lab. SOUPS2015.

R. Shay, L. Bauer, N. Christin, L. Cranor, A. Forget, S. Komanduri, M. Mazurek, W. Melicher, S. Segreti, and B. Ur. A Spoonful of Sugar? The Impact of Guidance and Feedback on Password-Creation Behavior. CHI 2015.

Chandrasekhar Bhagavatula, Blase Ur, Kevin Iacovino, Su Mon Kywe, Lorrie Faith Cranor, Marios Savvides. Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption. USEC 2015, February 8, 2015.

Saranga Komanduri, Richard Shay, Lorrie Faith Cranor, Cormac Herley, and Stuart Schechter. Telepathwords: Preventing Weak Passwords by Reading Users' Minds. USENIX Security 2014. August 20-22, 2014, San Diego, CA, pp. 591-606.

Richard Shay, Saranga Komanduri, Adam L. Durity, Philip (Seyoung) Huh, Michelle L. Mazurek, Sean M. Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Can long passwords be secure and usable? In CHI 2014: Conference on Human Factors in Computing Systems, April 2014. ACM. [Video teaser]

M.L. Mazurek, S. Komanduri, T. Vidas, L. Bauer, N. Christin, L.F. Cranor, P.G. Kelley, R. Shay, and B. Ur. Measuring Password Guessability for an Entire University. ACM CCS 2013.

>> More passwords papers ...

User controllable security and privacy

Managing security and privacy policies is known to be a difficult problem. It is important that new user interfaces be developed to effectively and efficiently support lay users in understanding and managing security and privacy policies - their own as well as those implemented by systems and individuals with whom they interact. Solutions in this area have traditionally taken a relatively narrow view of the problem by limiting the expressiveness of policy languages or the number of options available in templates, restricting some decisions to specific roles within the enterprise,

etc. As systems grow more pervasive and more complex, and as demands for increasing flexibility and delegation continue to grow, it is imperative to take a more fundamental view that weaves together issues of security, privacy and usability to systematically evaluate key tradeoffs between expressiveness, tolerance for errors, burden on users and overall user acceptance; and develop novel mechanisms and technologies that help mitigate these tradeoffs, maximizing accuracy and trustworthiness while minimizing the time and effort required by end users. The objective of this project is to develop new interfaces that combine user-centered design principles with dialog, explanation and learning technologies to assist users in specifying and refining policies. One new policy authoring interface we have developed is a visualization technique for displaying policies in a two-dimensional "expandable grid". (See also the User controllable security and privacy project page, the Expandable grids project, Grey project, Usable security for digital home storage and Locaccino.)

Recent papers

P. Klemperer, Y. Liang, M. Mazurek, M. Sleeper, B. Ur, L. Bauer, L.F. Cranor, N. Gupta, and M. Reiter. Tag, You Can See It! Using Tags for Access Control in Photo Sharing. CHI 2012.

K. Vaniea, L. Bauer, L.F. Cranor, and M.K. Reiter. Studying access control usability in the lab: Lessons learned from four studies. In *LASER 2012–Learning from Authoritative Security Experiment Results*, July 2012.

K. Vaniea, L. Bauer, L.F. Cranor, and M.K. Reiter. Out of sight, out of mind: Effects of displaying access-control information near the item it controls. In *Proceedings of the Tenth Annual Conference on Privacy, Security and Trust*, July 2012.

M. Mazurek, J.P. Arsenault, J. Bresee, N. Gupta, I. Ion, C. Johns, D. Lee, Y. Liang, J. Olsen, B. Salmon, R. Shay, K. Vaniea, L. Bauer, L.F. Cranor, G.R. Ganger, and M.K. Reiter. Access Control for Home Data Sharing: Attitudes, Needs and Practices. CHI 2010.

>> **More user-controllable security and privacy papers ...**

Usable Cyber Trust Indicators

When systems rely on a "human in the loop" to carry out a security-critical function, cyber trust indicators are often employed to communicate when and how to perform that function. Cyber trust indicators typically serve as warnings or status indicators that communicate information, remind users of information previously communicated, and influence user behavior. They include a variety of security- and privacy-related symbols in the operating system status bar or browser chrome, pop-up alerts, security control panels, or symbols embedded in web content. However, a growing body of literature has found the effectiveness of many of these indicators to be rather disappointing. It is becoming increasingly apparent that humans are a major cause of computer security failures and that security warnings and other cyber trust indicators are doing little to prevent humans from making security errors. In some cases, it may be possible to redesign systems to minimize the need for humans to perform security-critical functions, thus reducing or eliminating the need for security warnings. However, in

many cases it may be too expensive or difficult to automate security-critical tasks, and systems may need to rely on human judgment. In these cases, it is important to situate security indicators both spatially and temporally to maximize their effectiveness, and to design them to communicate clearly to users. The goal of this research is to systematically study the effectiveness of cyber trust indicators and develop approaches to making these indicators most effective and usable. We are currently focusing on security warning dialogs. See also our work on privacy indicators on our privacy decision making research page.

Recent papers

C. Bravo-Lillo, L. Cranor, S. Komanduri, S. Schechter, M. Sleeper. Harder to Ignore? Revisiting Pop-Up Fatigue and Approaches to Prevent It. SOUPS 2014.

C. Bravo-Lillo. Improving Computer Security Dialogs: An Exploration of Attention and Habituation PhD Thesis, Engineering & Public Policy Department, Carnegie Mellon University, Pittsburgh, PA, May 2014.

C. Bravo-Lillo, L.F. Cranor, J. Downs, S. Komanduri, R.W. Reeder, S. Schechter, and M. Sleeper. Your Attention Please: Designing security-decision UIs to make genuine risks harder to ignore. In Proceedings of the Eight Symposium On Usable Privacy and Security (SOUPS '13), Newcastle, United Kingdom, 2013.

L. Bauer, C. Bravo-Lillo, L. Cranor, and E. Fragkaki. Warning Design Guidelines. CMU-CyLab-13-002. February 5, 2013.

C. Bravo-Lillo, L. Cranor, J. Downs, S. Komanduri, S. Schechter, and M. Sleeper, Operating system framed in case of mistaken identity: Measuring the success of web-based spoofing attacks on OS password-entry dialogs, in Proceedings of the 19th ACM Conference on Computer and Communications Security, ACM, 18 October 2012.

C. Bravo-Lillo, L.F. Cranor, J.S. Downs, S. Komanuri. Bridging the Gap in Computer Security Warnings: A Mental Model Approach. *IEEE Security & Privacy,* 2011: 18-26.

>> More usable cyber trust indicators papers ...

Earlier Projects

Looking for some of our work that you can't find under "current projects"? Check here for our past projects.

Supporting trust decisions

When Internet users are asked to make "trust" decisions they often make the wrong decision. Implicit trust decisions include decisions about whether or not to open an email attachment or provide information in response to an email that claims to have been sent by a trusted entity. Explicit trust decisions are decisions made in response to specific trust- or security-related prompts such as pop-up boxes that ask the user whether to trust an expired certificate, execute downloaded software, or allow macros

to execute. Attackers are able to take advantage of most users' poor trust decision-making skills through a class of attacks known as "semantic attacks." It is not always possible for systems to make accurate trust decisions on a user's behalf, especially when those decisions require knowledge of contextual information. The goal of this research is not to make trust decisions for users, but rather to develop approaches to support users when they make trust decisions. Our research began with a mental models study aimed at understanding and modeling how people make trust decisions in the online context and ultimately resulted in the development of anti-phishing training tools and filtering software. The tools developed by this project our being commercialized by Wombat Security. For our publications, see the Supporting trust decisions project page.

Usable anonymity tools

A variety of tools have been developed to provide anonymity for various types of online interactions. Most of the work in this area has focused on improving the anonymity properties of these tools, and little has been done to improve their usability. We have been working on developing more usable interfaces for Tor.

FoxTor design document, our entry for the Tor GUI competition (selected as the phase 1 winner)

FoxTor download and FAQ

Other Selected Publications

M. Sleeper, A. Acquisti, L. Cranor, P. Kelley, S. Munson, NM. Sadeh. I Would Like To..., I Shouldn't..., I Wish I...: Exploring Behavior-Change Goals for Social Networking Sites. CSCW 2015: 1058-1069, Vancouver, BC, CA, March 14-18, 2015.

J. Wiese, A.J. Brush, T. Scott Saponas. Phoneprioception: enabling mobile phones to infer where they are kept. CHI 2013.

T. Vidas, E. Owusu, S. Wang, C. Zeng, and L. Cranor. QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks, USEC 2013 [originally published as CyLab Technical Report CMU-CyLab-12-022, November 2012].

M. Sleeper, D. Sharma, and L. Cranor. I Know Where You Live: Analyzing Privacy Protection in Public Databases. cmu-cylab-11-015, October 2011. [Extended version of paper presented at WPES 2011]

H. Hibshi, T. Vidas, and L. Cranor. Usability of Forensics Tools: A User Study. IT Security Incident Management and IT Forensics (IMF), 10-12, May 2011.

Janne Lindqvist, Justin Cranshaw, Jason Wiese, Jason Hong, and John Zimmerman. I'm the Mayor of My House: Examining Why People Use foursquare - a Social-Driven Location Sharing Application. In CHI 2011: Conference on Human Factors in Computing Systems, May 2011.

Timothy Vidas, Nicolas Christin, Lorrie Cranor. Curbing Android Permission Creep. Web 2.0 Security & Privacy 2011. Oakland, CA, May 26, 2011.

S. Garfinkel and L. Cranor. Institutional Review Boards and Your Research. *Communications of the ACM,* June 2010, p. 38-40. DOI = http://doi.acm.org/10.1145/1743546.1743563

J. Downs, M. Holbrook, S. Sheng, and L. Cranor. Are Your Participants Gaming the System? Screening Mechanical Turk Workers. CHI 2010.

Sarah Spiekermann and Lorrie Faith Cranor. Engineering Privacy. *IEEE Transactions on Software Engineering*. Vo. 35, No. 1, January/February, 2009, pp. 67-82.

Ahren Studer, Christina Johns, Jaanus Kase, Kyle O'Meara, Lorrie Cranor. A Survey to Guide Group Key Protocol Development. Annual Computer Security Applications Conference (ACSAC) 2008, December 8-12, 2008, Anaheim, CA.

A. McDonald and L. Cranor. How Technology Drives Vehicular Privacy. I/S: A Journal of Law and Policy for the Information Society Volume 2, Issue 3 (2006).

X. Sheng and L. Cranor. An Evaluation of the Effectiveness of US Financial Privacy Legislation Through the Analysis of Privacy Policies. I/S: A Journal of Law and Policy for the Information Society, Volume 2, Number 3, Fall 2006, pp. 943-979.

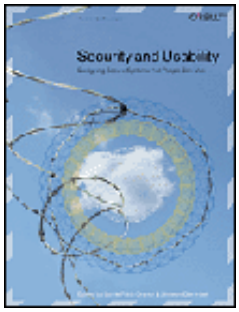
L. Cranor. 'I Didn't Buy it for Myself': Privacy and Ecommerce Personalization. *Proceedings of the 2nd ACM Workshop on Privacy in the Electronic Society*, October 30, 2003, Washington, DC.

L. Cranor, J. Hong, and M. Reiter. Teaching Usable Privacy and Security: A guide for instructors. 2007.

S. Egelman and L. Cranor. The Real ID Act: Fixing Identity Documents with Duct Tape. *I/S: A Journal of Law and Policy for the Information Society*, Volume 2, Number 1, Winter 2006, pp. 149-183.

M. Geiger and L. Cranor, Counter-Forensic Privacy Tools: A Forensic Evaluation. ISRI Technical Report. CMU-ISRI-05-119, 2005.

Romanosky, S., Acquisti, A., Hong, J., Cranor, L. F., and Friedman, B. 2006. Privacy patterns for online interactions. In Proceedings of the 2006 Conference on Pattern Languages of Programs (Portland, Oregon, October 21 - 23, 2006). PLoP '06. ACM, New York, NY, 1-9.



Resources

Join our cups-friends mailing list for announcements about our papers and events and discussions about usable privacy and security

Security and Usability: Designing Secure Systems that People Can Use, edited by Lorrie Cranor and Simson Garfinkel, is now available

L. Cranor, J. Hong, and M. Reiter. Teaching Usable Privacy and Security: A guide for instructors. 2007.

The HCISec Bibliography contains a good list of CUPS-related publications.

HCISEC mailing list

Usable Security Blog from UC Berkeley

Slides are available from the July 2004 Workshop on Usable Privacy and Security Software

Usability, Psychology, and Security workshop

Vizsec - a research and development community interested in applying information visualization techniques to the problems of

computer security

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation or any of our other funders.

Privacy policy